Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/FR05/000648

International filing date: 17 March 2005 (17.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/600,912
Filing date: 12 August 2004 (12.08.2004)

Date of receipt at the International Bureau: 27 June 2005 (27.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PA 1299365

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 25, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: *60/600,912*
FILING DATE: *August 12, 2004*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

E. BORNETT
Certifying Officer

By Express Mail # EV514454583US

PROVISIONAL APPLICATION COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR 1.53(b)(2).

Docket #: 33900-159P	Type a plus sign (+) inside this box→	+

INVENTOR(S)/APPLICANT(S)

NAME *(First, Middle, Last)*	RESIDENCE *(City and either State or Country)*
Philippe BRESSY Gilles PERROTEY	Ollioules, France Gemenos, France

TITLE OF THE INVENTION *(280 characters max)*

Procédé et dispositif de sécurisation de l'accès à un périphérique

CORRESPONDENCE ADDRESS

Lance J. Lieberman, Esq.
(212) 687-2770

Cohen, Pontani, Lieberman & Pavane
551 Fifth Avenue, Suite 1210
New York, New York 10176

ENCLOSED APPLICATION PARTS *(check all that apply)*

[x]	Specification	*Number of Pages* [28]	[]	Other *(specify):*
[x]	Drawing(s)	*Number of Sheets* [6]		

METHOD OF PAYMENT *(check one)*

[x]	A check is enclosed to cover the Provisional filing fees	PROVISIONAL FILING FEE AMOUNTS: $80
[x]	**If no check is enclosed or the enclosed check is insufficient** - The Commissioner is hereby authorized to charge the filing fees or credit any overpayment to Deposit Acct. No. 03-2412.	

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government

[x] No
[ ] Yes, the name of the U.S. Government agency and the Government contract number are: _
[x] Small Entity Status is claimed

Respectfully submitted,

Dated: August 12, 2004

By: _____
Lance J. Lieberman
Reg. No. 28,437

COHEN, PONTANI, LIEBERMAN & PAVANE
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

PROVISIONAL APPLICATION FILING ONLY

Rev. Jun-02

La présente invention se situe dans le domaine de la sécurisation des appareils électroniques, et plus précisément dans celui de la protection de ces appareils contre des manipulations frauduleuses et des attaques à leur intégrité.

On connaît principalement deux types d'attaque, à savoir les attaques de type logiciel d'une part et celles par ajout ou substitution de composants matériels d'autre part.

Pour parer aux attaques logicielles, on connaît des outils dits de haut niveau, c'est-à-dire opérant au-dessus des couches du système d'exploitation (antivirus, pare-feu, etc.).

Malheureusement, ces outils même performants, présentent une fragilité importante dans le sens où ils peuvent être désactivés ou contournés avant même leur chargement en mémoire.

Un consortium nommé « Trusted Computing Group » (TCG) vise à palier cet inconvénient en fournissant des outils et des méthodes de protection des couches logicielles basses.

TCG propose en particulier une méthode de vérification de l'authenticité du BIOS (Basic Input Output System) d'un ordinateur personnel avant son lancement.

Une telle méthode utilise à cette fin un code de confiance CRTM (Core Root of Trust Measurement en anglais), ce code CRTM étant exécuté à la mise sous tension de l'ordinateur pour calculer une signature du BIOS.

Ce code de confiance CRTM constitue ainsi la base de toute la chaîne de sécurité logicielle dans l'équipement, et doit donc être protégé lui aussi contre les attaques.

Afin d'assurer la protection de ce code CRTM, il est traditionnellement prévu d'implémenter celui-ci dans un secteur spécifique d'une mémoire de type flash installée sur la carte mère de l'équipement.

L'inconvénient d'une telle solution est que la modification de ce code de confiance CRTM, pour une mise à jour par exemple, est impossible sans intervention physique sur la carte mère, comme le décrit le document IBM US 2003/0135727 publié le 17 juillet 2003.

Ce document propose une première solution à ce problème consistant à implémenter le code de confiance (CRTM) dans une carte accessoire à la carte

mère (feature card en anglais), cette carte accessoire comportant son propre BIOS. Les mises à jour peuvent alors s'effectuer simplement par remplacement physique de cette carte accessoire.

Si cette solution est acceptable dans le cadre des spécifications élaborées par TCG, on comprend qu'elle ne l'est plus du tout lorsque l'on veut étendre la protection des boot loader et des BIOS au second type d'attaques, les attaques matérielles, du fait d'un utilisateur ou d'un tiers (console de jeux, code IMEI et SIM lock des GSM notamment).

Cette solution présente en effet un inconvénient majeur pour ce cas de protection étendue, puisqu'il suffit de retirer cette carte accessoire pour désactiver l'ensemble des fonctions de sécurité de l'équipement.

La demanderesse s'est attachée à résoudre le problème précité en le généralisant à tout appareil électronique, à savoir rendre possible la modification, dans le but de mise à jour, du code de démarrage (boot loader) dans la mémoire flash sans intervention physique, tout en protégeant ce code des manipulations frauduleuses (remplacement, modification).

La demanderesse propose une solution au problème précédent basée sur le contrôle de l'accès en écriture à la mémoire flash comportant le code de démarrage.

D'une façon plus générale, ce problème consiste à contrôler l'accès à une mémoire ou un périphérique d'un processeur, que celui ci soit embarqué ou non dans le processeur.

A cet effet, l'invention consiste à utiliser un programme informatique constituant un point unique d'accès au périphérique, préférentiellement situé dans une zone sûre et contrôlée du processeur, et contrôlant en coopération avec une unité matérielle, le signal électrique d'accès à ce périphérique.

Plus précisément, et selon un premier aspect, l'invention vise une unité matérielle de contrôle d'accès à un périphérique.

Cette unité matérielle comporte :

- des moyens d'obtention d'un code d'autorisation d'accès au périphérique ;

- des moyens de comparaison de ce code d'autorisation d'accès avec une valeur de référence prédéterminée ; et

By Express Mail
No. EV514454583US

- des moyens, dits de validation, adaptés à générer un signal électrique de validation d'un signal électrique d'accès à ce périphérique en fonction du résultat de cette comparaison.

L'invention permet ainsi de contrôler l'accès au périphérique d'un processeur en validant au plus bas niveau, et de façon matérielle, le signal électrique d'accès à ce périphérique. Ce périphérique peut notamment être choisi parmi un écran, un clavier, une mémoire, un contrôleur d'une interface de communication, une unité de gestion mémoire (MMU) ou une unité de protection de mémoire (MPU).

Dans la suite de ce document, nous appellerons "périphérique" tout type de composant électronique (écran, clavier, mémoire, interface de communication, interface de carte à puce, MMU, MPU, ...), que ceux-ci soient discrets où "intégrés" dans des FPGA ou ASIC.

De même, nous appellerons "signal électrique d'accès" tout signal électrique devant être activé pour la sélection (signal de type « ChipSelect », CS) du périphérique ou l'écriture (signal de type "WRITE-ENABLE", WE) sur ce périphérique.

Conformément à la présente invention, un accès au périphérique ainsi protégé n'est possible que sur présentation à l'unité matérielle de contrôle d'accès audit périphérique d'un code d'autorisation d'accès compatible avec la valeur de référence prédéterminée connue de cette unité matérielle.

L'invention permet ainsi notamment la protection d'une mémoire dite sécurisée, du type par exemple de celle contenue dans un téléphone mobile conforme à la norme GSM pour la mémorisation des conditions commerciales souscrites par abonnement avec un opérateur (SIM Lock).

La substitution frauduleuse de ces règles SIM-Lock ne devient possible que sur présentation d'un code d'autorisation d'accès valide à l'unité matérielle de contrôle de l'accès à cette mémoire.

L'invention permet aussi de mettre à jour le BIOS ou le système d'exploitation d'un appareil, à distance. On pourra donc aisément mettre à jour les téléphones portables, et ce, directement avec la liaison sans fil GSM, sans que le client ne se déplace vers un centre de mise à jour.

By Express Mail
No. EV514454583US

L'invention peut ainsi être utilisée pour empêcher toute modification frauduleuse du BIOS d'un PC, ce qui augmente grandement la sécurité de ce PC, notamment quand le BIOS contient des mécanismes de sécurité de plus haut niveau.

Préférentiellement, l'unité matérielle de contrôle d'accès selon l'invention comporte des moyens de déclenchement d'une interruption non masquable d'alarme, lorsque le code d'autorisation d'accès est différent de la valeur de référence prédéterminée.

Cette caractéristique permet ainsi, par traitement de cette interruption d'alarme, d'empêcher toute attaque dite « en force brute », à savoir des attaques consistant à présenter des code d'autorisation d'accès, jusqu'à la présentation d'un code fortuitement identique à la valeur de référence prédéterminée.

Dans une première variante de réalisation, la valeur de référence prédéterminée est une constante.

Cette variante est particulièrement simple à mettre en œuvre. Elle permet déjà de se prémunir contre toute attaque venant d'un tiers qui ne connaîtrait pas la constante précitée.

Dans une deuxième variante de réalisation, l'unité matérielle de contrôle d'accès selon l'invention comporte des moyens de génération de la valeur de référence précitée selon une loi prédéterminée.

Cette caractéristique permet avantageusement de renforcer le contrôle d'accès au périphérique car seul un pirate connaissant la loi prédéterminée pourrait être en mesure de présenter un code d'autorisation d'accès valide à l'unité matérielle de contrôle d'accès.

Dans un mode préféré de cette deuxième variante de réalisation, la valeur de référence prédéterminée est un compteur initialisé à la mise sous tension de l'unité matérielle, et la loi prédéterminée consiste à incrémenter ce compteur à chaque obtention du code d'autorisation d'accès.

La mise en œuvre de cette loi prédéterminée peut notamment être réalisée par un compteur associé à un automate d'états finis, ce qui évite l'utilisation plus onéreuse d'un (co-)processeur, et limite le coût de fabrication de l'unité matérielle dans son ensemble.

By Express Mail
No.
EV514454583US

Dans un mode de réalisation préféré, l'unité matérielle conforme à l'invention comporte :

- des moyens de déclenchement d'une interruption non masquable de contrôle et ;
- des moyens d'obtention du code d'autorisation d'accès (Code-AA) précité consécutivement à ce déclenchement.

Cette caractéristique permet de renforcer le contrôle d'accès au périphérique car elle permet de s'assurer que le code d'autorisation d'accès est reçu de façon certaine en provenance d'un organe de confiance constitué par la routine d'interruption de contrôle.

Dans la première variante de réalisation précitée, la routine d'interruption de contrôle peut ainsi autoriser l'accès au périphérique en envoyant simplement la constante, à l'unité matérielle de contrôle.

Selon une autre caractéristique avantageuse, les moyens de validation de l'unité matérielle de contrôle d'accès au périphérique comportent des moyens de combinaison logique adaptés à :

- recevoir un signal électrique de demande d'accès à ce périphérique ;
- recevoir le signal de validation; et
- valider le signal électrique d'accès en fonction d'un état du signal électrique de demande d'accès, d'un état du signal de validation, et d'une logique représentée dans une table de vérité.

Selon cette caractéristique, on valide ainsi l'accès au périphérique lorsque deux conditions sont réunies, à savoir d'une part la présence d'une demande d'accès au périphérique par un composant tiers, par exemple un processeur, et d'autre part lorsque le résultat des comparaisons précitées est représentatif de l'obtention d'un code d'autorisation d'accès valide par l'unité matérielle du contrôle.

Préférentiellement, le signal d'accès résulte de la combinaison "ET logique" entre le signal de demande d'accès et le signal de validation. Ce moyen de réalisation est particulièrement aisé à mettre en œuvre.

Dans un mode préféré de réalisation, l'unité matérielle de contrôle d'accès selon l'invention, comporte des moyens de lecture d'un état du signal électrique de demande d'accès, et des moyens de déclenchement d'une interruption non

By Express Mail
No. EV514454583US

masquable d'alarme en fonction de cet état et de l'état du signal électrique de validation d'accès.

Cette caractéristique permet avantageusement de déclencher une interruption non masquable d'alarme, lorsque l'état du signal électrique de demande d'accès est représentatif d'une demande d'accès au périphérique, sans qu'un code d'autorisation d'accès n'ait été présenté à l'unité matérielle de contrôle d'accès.

Dans un mode préféré de réalisation, l'unité matérielle de contrôle d'accès selon l'invention comporte des moyens d'inhibition du signal de validation, cette inhibition étant préférentiellement effectuée consécutivement à un ou plusieurs accès au périphérique.

Cette caractéristique permet avantageusement de renforcer le contrôle d'accès au périphérique, puisque celui-ci doit s'exercer régulièrement, voire même avant chaque accès au périphérique.

Dans un autre mode de réalisation, l'inhibition du signal de validation est effectuée après un délai prédéterminé compté à partir de la génération du signal électrique de validation d'accès, où à partir de l'obtention du code d'accès.

Cette caractéristique permet avantageusement d'autoriser l'accès au périphérique sans contrôle durant ce délai, ce qui améliore les performances globales du système. Cette caractéristique est particulièrement intéressante lorsque le volume de données échangées avec ce périphérique est important comme dans le cas d'un écran.

Corrélativement, l'invention vise un procédé de contrôle d'accès à un périphérique, ce procédé comportant les étapes suivantes :

- obtention d'un code d'autorisation d'accès au périphérique ;
- comparaison du code d'autorisation d'accès avec une valeur de référence prédéterminée ;
- génération d'un signal électrique de validation d'un signal d'accès au périphérique en fonction du résultat de cette étape de comparaison.

Préférentiellement, le procédé de contrôle d'accès selon l'invention comporte en outre :

- une étape de déclenchement d'une interruption non masquable de contrôle; et

- une étape d'obtention du code d'accès consécutivement audit déclenchement.

Comme décrit précédemment, cette caractéristique permet de renforcer le contrôle d'accès au périphérique car elle permet de s'assurer que le code d'autorisation d'accès est reçu de façon certaine en provenance d'un organe de confiance constitué par la routine d'interruption de contrôle.

Préférentiellement, l'étape de déclenchement d'une interruption non masquable de contrôle est effectuée consécutivement à une étape d'obtention d'un code de déclenchement ;

Cette caractéristique permet encore de renforcer le contrôle d 'accès au périphérique car elle sollicitation de l'unité matérielle de contrôle d'accès par un tiers qui ne connaîtrait pas le code de déclenchement aboutirait à un déclenchement d'alarme.

Les avantages et caractéristiques particuliers de ce procédé de contrôle d'accès étant les mêmes que ceux décrits précédemment en référence à l'unité matérielle de contrôle, ils ne seront pas rappelés ici. Ce procédé consiste essentiellement à vérifier la validité d'un ou plusieurs code d'autorisation d'accès en le comparant à des valeurs de référence prédéterminées (constantes ou générées selon une loi), et à valider un signal électrique d'accès au périphérique en fonction de cette comparaison.

Selon un autre aspect, l'invention concerne un processeur comportant une unité matérielle de contrôle d'accès telle que décrite brièvement ci-dessus.

Dans un mode préféré de réalisation, ce processeur selon l'invention comporte en outre des moyens d'envoi du code d'autorisation d'accès à l'unité matérielle de contrôle d'accès.

Dans ce mode préféré de réalisation de l'invention, l'unité matérielle de contrôle d'accès décrite précédemment est embarquée au sein d'un processeur, ce processeur comportant des moyens d'envoi à l'unité matérielle de contrôle, du code d'autorisation d'accès à un périphérique donné.

Ce mode préféré de réalisation de l'invention renforce considérablement le contrôle de l'accès à ce périphérique, car il devient alors impossible de contourner physiquement, ou autrement dit de shunter, l'unité matérielle de contrôle d'accès.

Préférentiellement, le processeur selon l'invention comporte le périphérique auquel il protège l'accès.

Ce périphérique peut notamment être une unité de gestion de mémoire.

L'invention peut protéger ainsi l'accès à l'unité de gestion de la mémoire (MMU). Ceci permet de créer deux environnements systèmes rigoureusement étanches sur un même processeur. Si de plus, on assure un espace d'échanges de données contrôlées entre ces deux environnements, l'homme du métier comprendra que l'on peut aisément construire des appareils dont certaines fonctions (système d'exploitation ou applications sensibles de type paiement, authentification, protection des droits des auteurs et de la copie) sont isolées des applications plus ouvertes et donc plus sensibles aux attaques (Browser Internet, chargement de jeux, de vidéo, email etc..).

Le périphérique contenu dans le processeur selon l'invention peut également être un contrôleur d'écriture dans la mémoire d'amorçage du processeur.

Ce mode préféré de réalisation permet ainsi de sécuriser la mémoire d'amorçage du processeur, cette protection rendant impossible la modification frauduleuse des données contenues dans cette mémoire, zone dont la sécurité est très critique en ce qu'elle héberge souvent des appels à des procédures de sécurisation de plus haut niveau.

Corrélativement, l'invention concerne un procédé de gestion d'accès à un périphérique. Ce procédé comporte une étape de mise en œuvre d'une routine de contrôle associée à une interruption non masquable de contrôle, ladite routine comportant une étape d'envoi d'un code d'autorisation d'accès à une unité matérielle de contrôle d'accès telle que décrite brièvement ci-dessus.

Dans une première variante de réalisation, le code de contrôle d'accès est une constante, lue à partir d'une mémoire protégée.

Dans une deuxième variante de réalisation, le procédé de gestion d'accès comporte en outre une étape de génération d'un code d'autorisation d'accès selon une loi prédéterminée.

L'homme du métier comprendra aisément qu'il est nécessaire, dans cette première variante de réalisation, de masquer toutes les interruptions, sans quoi un accès illicite au périphérique pourrait être effectué par une interruption mal

intentionnée dans l'intervalle de temps compris entre la lecture de la constante dans la mémoire protégée et le déclenchement de la routine d'interruption non masquable de contrôle.

Les avantages et caractéristiques particuliers de ce procédé de gestion d'accès étant les mêmes que ceux décrits brièvement ci-dessus en référence au processeur selon l'invention, ils ne sont pas rappelés ici. Ce procédé consiste essentiellement à fournir, en provenance d'un organe de confiance (à savoir le processeur mettant en œuvre la routine d'interruption de contrôle) des codes d'autorisation d'accès, ces codes étant comparés par l'unité matérielle de contrôle avec des valeurs de référence prédéterminées (constantes ou générées selon une loi) pour autoriser ou non l'accès au périphérique.

L'invention vise aussi un programme informatique comportant une instruction d'accès à un périphérique et une instruction d'envoi d'un code de déclenchement à une unité matérielle de contrôle d'accès à ce périphérique telle que décrite brièvement ci-dessus, préalablement à l'exécution de cette instruction d'accès.

Préférentiellement, ce programme informatique comporte en outre des moyens de génération du code de déclenchement selon la loi prédéterminée de génération du code d'autorisation d'accès.

Ce programme informatique constitue un point unique d'accès au périphérique, préférentiellement situé dans une zone sûre et contrôlée du processeur. Ce programme contrôle, en coopération avec l'unité matérielle, le signal électrique d'accès à ce périphérique.

L'invention vise aussi un processeur adapté à mettre en œuvre un procédé de contrôle d'accès, un procédé de gestion d'accès, et/ou un programme informatique tels que décrits brièvement ci-dessus.

D'autres aspects et avantages de la présente invention apparaîtront plus clairement à la lecture du mode particulier de réalisation qui va suivre, cette description étant donnée uniquement à titre d'exemple non limitatif et faite en référence aux dessins annexés, sur lesquels :

- la figure 1 représente un processeur conforme à l'invention dans un premier mode de réalisation,

- la figure 2 représente un processeur conforme à l'invention dans un deuxième mode de réalisation,

- la figure 3 représente une unité matérielle de contrôle d'accès conforme à l'invention dans un mode préféré de réalisation,

- les figures 4a à 4d représentent sous forme d'automates, les principales étapes de procédés de contrôle d'accès conformes à l'invention,

- la figure 5 représente sous forme d'organigramme, les principales étapes d'une routine d'interruption de contrôle conforme à l'invention dans un mode préféré de réalisation ; et

- la figure 6 représente, sous forme d'organigramme, les principales étapes d'un programme accédant à un périphérique protégé, conformément à la présente invention.

L'exemple de réalisation de l'invention décrit ici concerne plus particulièrement la protection de l'accès à une mémoire d'amorçage contenue dans un processeur.

La **figure 1** représente un processeur 110 conforme à l'invention dans un mode préféré de réalisation.

Le processeur 110 comporte une mémoire d'amorçage 120 (en anglais BOOT-ROM) et une mémoire volatile RAM protégée. Cette mémoire d'amorçage 120 comporte une table de vecteurs d'interruption VECT, deux routines d'interruption, respectivement de contrôle IRT1 et d'alarme IRT2, et un programme informatique PROG.

Ce programme informatique PROG est un programme de contrôle d'un périphérique P interne au processeur, un tel programme étant habituellement connu sous le nom de pilote (en anglais : « driver »).

Dans le mode préféré de réalisation décrit ici, le périphérique P interne au processeur est un contrôleur d'écriture pour la mémoire d'amorçage 120 précitée.

Le processeur 110 comporte une unité matérielle 20 de contrôle d'accès au périphérique P, conforme à la présente invention.

Cette unité matérielle de contrôle d'accès 20 comporte des moyens d'obtention d'un code Code-DD de déclenchement et d'un code Code-AA d'autorisation d'accès au périphérique P.

By Express Mail
No. EV514454583US

Dans le mode de réalisation décrit ici, le code de déclenchement Code-DD et le code d'autorisation d'accès Code-AA sont obtenus dans un même registre 21.

Dans le mode préféré de réalisation décrit ici :

- le code Code-AA d'autorisation d'accès est écrit dans le registre 21 par la routine d'interruption de contrôle IRT1 ; et

- et le code de déclenchement Code-DD est écrit dans le registre 21 par le pilote PROG du périphérique P.

En effet, conformément à l'invention, avant chaque instruction (WRITE, READ,...) d'accès au périphérique P, le programme informatique PROG écrit un code de déclenchement Code-DD dans le registre 21 de l'unité matérielle 20.

Dans le mode de réalisation décrit ici, le code de déclenchement Code-DD et le code d'autorisation d'accès Code-AA sont deux valeurs successives d'une même variable calculées selon la loi d'incrémentation prédéterminée.

Cette variable est mémorisée dans une zone protégée de la volatile RAM du processeur. Cette mémoire n'est accessible qu'au programme informatique PROG et à la routine d'interruption de contrôle IRT1.

L'unité matérielle de contrôle d'accès 20 comporte également des moyens 24 adaptés à générer, selon une loi prédéterminée, une valeur de référence Code-UMCA lorsqu'un code d'autorisation Code-AA ou un code de déclenchement Code-DD est écrit dans le registre 21.

Dans le mode préféré de réalisation décrit ici, cette loi consiste à incrémenter le compteur Code-UMCA, celui-ci étant initialisé à la mise sous tension du processeur 110.

L'unité matérielle de contrôle d'accès 20 comporte également des moyens 22 de comparaison du code d'autorisation d'accès Code-AA (et du code de déclenchement Code-DD) obtenu dans le registre 21 avec la valeur de référence prédéterminée Code-UMCA, calculée par les moyens 24 de génération de cette valeur.

Dans le mode préféré de réalisation décrit ici, ces moyens de comparaison 22 sont constitués par une logique câblée.

Quoiqu'il en soit, ces moyens de comparaison 22 sont adaptés à envoyer un premier signal à une unité 26 de déclenchement d'une interruption non

masquable, lorsque le code de déclenchement Code-DD est comparé égal à la valeur courante du code de référence Code-UMCA. Ceci sera décrit ultérieurement en référence à la figure 4a.

Sur réception de ce premier signal, les moyens 26 de déclenchement d'une interruption non masquable génèrent un signal d'interruption non masquable NMI1.

Sur réception de ce signal d'interruption non masquable NMI1, le processeur exécute, grâce à la table de vecteur d'interruption VECT, la routine d'interruption de contrôle IRT1.

Cette routine d'interruption de contrôle IRT1 met en œuvre une fonction informatique Gen-Code adaptée à calculer une nouvelle valeur du code d'autorisation d'accès Code-AA selon une loi prédéterminée, à mémoriser cette nouvelle valeur dans la mémoire protégée, et à écrire cette nouvelle valeur Code-AA dans le registre 21 de l'unité matérielle de contrôle d'accès 20.

Cette loi prédéterminée est identique à celle mise en œuvre par les moyens 24 de génération de la valeur de référence Code-UMCA. Ainsi, dans le mode de réalisation préféré décrit ici, cette loi est une loi d'incrémentation et le code d'autorisation d'accès Code-AA est égal à la valeur du code de déclenchement Code-DD plus un.

Lorsque les moyens 21 d'obtention du code d'autorisation d'accès Code-AA reçoivent ce code d'autorisation Code-AA en provenance de la routine d'interruption IRT1 de contrôle, les moyens 24 de génération d'une valeur de référence Code-UMCA génèrent une nouvelle valeur de référence selon la loi prédéterminée d'incrémentation.

Ces deux nouvelles valeurs sont alors comparées par les moyens 22 de comparaison décrits précédemment.

Conformément à l'invention, les moyens 22 de comparaison sont adaptés à positionner une valeur représentative du résultat de la comparaison de ces deux nouvelles valeurs dans une bascule 23 de l'unité matérielle de contrôle d'accès 20.

Dans l'exemple de réalisation décrit ici, nous supposerons que la logique câblée 22 positionne la valeur 1 dans la bascule 23 lorsque le nouveau code

d'autorisation d'accès Code-AA et la nouvelle valeur de référence prédéterminée Code-UMCA sont égaux.

Ainsi, dans ce mode préféré de réalisation décrit ici, le contenu de la bascule 23 est positionné à 1 lorsque les codes de déclenchement Code-DD et d'autorisation Code-AA reçus successivement en provenance du pilote PROG et de la routine d'interruption de contrôle IRT1 sont égaux aux deux valeurs de référence code–UMCA prédéterminées générées par les moyens 24 sur réception des codes.

Conformément à ce mode préféré de réalisation, lorsque la bascule 23 est positionnée à 1, celle-ci génère un signal électrique de validation SIG-VAL à destination de moyens de combinaison logique 25 de l'unité matérielle de contrôle d'accès 20.

Ainsi dans ce mode préféré de réalisation , le signal de validation SIG-VAL est généré, lorsque les deux conditions précitées sont réunies.

Avant de transmettre le code de déclenchement Code-DD à l'unité matérielle de contrôle d'accès 20, le pilote PROG génère une nouvelle valeur selon la loi prédéterminée, c'est-à-dire dans le mode décrit ici, l'incrémente, et mémorise cette nouvelle valeur dans la mémoire volatile RAM protégée.

Le pilote du périphérique P exécute ensuite une instruction d'accès au périphérique P.

De façon connue de l'homme du métier, cette instruction génère, en sortie d'un décodeur d'adresse 27, un signal électrique d'accès, de type Chip-Select CS à destination du périphérique P.

Conformément à la présente invention, ce signal d'accès n'est pas directement transmis au périphérique P, mais vient en entrée des moyens de combinaison logique 25 précités.

Dans la suite de ce document, ce signal sera dénommé signal électrique de demande d'accès CS-RQ.

Les moyens de combinaison logique 25 qui reçoivent en entrée d'une part le signal électrique CS-RQ de demande d'accès au périphérique P et, d'autre part, le signal de validation SIG-VAL comportent également une table de vérité adaptée, de façon connue, à générer un signal d'accès de type « chip select » CS, à destination du périphérique P.

By Express Mail
No. EV514454583US

Cette table de vérité 25 permet en d'autres termes la validation du signal électrique d'accès au périphérique P, au sens de la présente invention.

Dans le mode préféré de réalisation décrit ici, le signal d'accès CS en sortie des moyens 25 de combinaison logique est fourni en entrée de la bascule 23.

Dans ce mode de réalisation, lorsqu'un accès au périphérique P est réalisé, c'est-à-dire lorsque l'état du signal d'accès CS est haut, la valeur de la bascule 23 est remise à 0.

Ceci a pour effet d'inhiber le signal de validation SIG-VAL en sortie de cette même bascule 23 et donc d'invalider tout accès au périphérique P.

Dans un autre mode de réalisation, le signal de validation SIG-VAL est inhibé non pas à chaque accès au périphérique P, mais de façon cyclique, par exemple tous les cinq accès.

Dans un autre mode de réalisation préféré, le signal d'accès CS n'est pas rebouclé sur la bascule 23, celle-ci étant adaptée à inhiber automatiquement le signal de validation SIG-VAL après un délai prédéterminé compté à partir de la génération de ce même signal, ou à partir de l'obtention du code de déclenchement Code-DD.

Dans le mode préféré de réalisation décrit ici, les moyens de comparaison 22 sont adaptés à envoyer un deuxième signal à l'unité 26 de déclenchement d'une interruption non masquable lorsqu'elle détecte, par comparaison, qu'un code obtenu dans le registre 21 est différent de la valeur de référence prédéterminée Code-UMCA générée sur réception de ce code.

Sur réception de ce deuxième signal, les moyens 26 de déclenchement d'une interruption non masquable envoient un deuxième signal d'interruption NMI2 à la mémoire d'amorçage 120.

Ainsi, si un programme hostile écrit un code aléatoire dans le registre 21, les moyens de comparaison 22 déclencheront une interruption non masquable NMI2.

Sur réception de ce deuxième signal d'interruption, le processeur exécute la routine d'interruption d'alarme IRT2 pour le traitement d'accès frauduleux au périphérique P.

La **figure 2** représente un autre processeur 210 conforme à la présente invention dans un autre mode de réalisation.

La seule différence entre ce processeur 210 et le processeur 110 décrit précédemment en référence à la figure 1, est que le processeur 210 est utilisé pour contrôler l'accès à un périphérique P externe.

Toutes les caractéristiques autres étant identiques, il ne sera pas décrit plus en avant ici.

La **figure 3** représente une unité matérielle de contrôle d'accès 20, sous forme d'un composant externe à un processeur 10.

Dans ce mode de réalisation de l'invention, le processeur 10 coopérant avec l'unité matérielle de contrôle d'accès 20, comporte une mémoire d'amorçage 120 identique à celle décrite précédemment en référence au processeur 110 de la figure 1.

L'unité matérielle de contrôle d'accès 20 de cette figure est identique à celle décrite précédemment en référence à la figure 1 et ne sera pas détaillée ci-après.

La **figure 4a** représente sous forme d'automate à états finis les principales étapes d'un procédé de contrôle d'accès conforme à l'invention dans un mode préféré de réalisation.

Sur cette figure, les « bulles » représentent des états, les flèches des transitions, et les rectangles des conditions nécessaires et suffisantes à la réalisation des transitions.

Dans la suite de la description, on emploiera indifféremment les terminologies « étape » ou « état » connues de l'homme du métier des programmes informatiques.

Cet automate comporte un premier état E10 d'initialisation, duquel on sort (transition E15) lorsque la valeur de référence prédéterminée Code-UMCA est initialisée avec une valeur initiale, par exemple zéro, puis mémorisée dans la mémoire volatile RAM.

On entre alors dans un état d'attente E20.

Lorsque dans cet état d'attente E20 l'unité matérielle de contrôle d'accès reçoit un code de déclenchement Code-DD (transition E25), on entre dans un

état E30 de comparaison de ce code de déclenchement Code-DD avec la valeur de référence prédéterminée Code-UMCA.

En revanche, lorsque dans cet état d'attente E20, on détecte un signal électrique de demande d'accès CS-RQ au périphérique P (transition E22), on entre dans un état E100 de déclenchement d'une interruption non masquable d'alarme NMI2.

On quitte automatiquement cet état E100 de déclenchement d'une interruption non masquable d'alarme NMI2, pour entrer dans un état E110 de gestion d'alarme.

Dans un mode de réalisation préféré, l'état E110 de gestion d'alarme entraîne l'exécution d'un code terminal, (génération d'une condition de RESET). Dans d'autres modes de réalisations, diverses réactions sont envisageables en fonction de l'application. Ces modes de réalisation ne sont pas l'objet de ce brevet et ne seront pas détaillés ici.

Une fois cette procédure de gestion d'alarme terminée, on peut effacer l'alarme et revenir dans l'état E20 d'attente décrit précédemment

Lorsque depuis l'état E30 de comparaison, on détermine que le code de déclenchement Code-DD est différent de la valeur de référence prédéterminée Code-UMCA (transition E85), on entre dans l'état E100 de déclenchement d'une interruption d'alarme non masquable NMI2 décrit précédemment.

En revanche, lorsque depuis l'état E30 de comparaison, on détermine que la valeur du code de déclenchement Code-DD est égale à la valeur de référence prédéterminée Code-UMCA (transition E31), on entre dans un état E32 de génération d'une nouvelle valeur de référence prédéterminée Code-UMCA selon la loi d'incrémentation prédéterminée.

Cet état E32 de génération d'une nouvelle valeur de référence Code-UMCA, est suivi d'un état E34 de déclenchement d'une interruption non masquable de contrôle NMI1.

Une fois cette interruption non masquable de contrôle NMI1 déclenchée, on entre dans un état E36 d'attente d'un code d'autorisation d'accès Code-AA.

Si dans cet état E36 d'attente d'un code d'autorisation d'accès code AA, on détecte un signal électrique de demande d'accès CS-RQ (transition E90) , on

entre dans l'état E100 de déclenchement d'une interruption d'alarme non masquable NMI2.

En revanche, lorsque dans l'état E36 d'attente, on obtient un code d'autorisation d'accès Code-AA (transition E37) , on entre dans un état E38 de comparaison de ce code d'autorisation d'accès Code-AA avec une nouvelle valeur de référence courante Code-UMCA.

Si au cours de cette état E38 de comparaison on détermine que le code d'autorisation d'accès Code-AA est différent de la valeur de référence Code-UMCA (transition E95), on entre dans l'état E100 de déclenchement d'une interruption non masquable d'alarme NMI2.

En revanche, si ces deux valeurs sont égales (transition E39), on sort de l'état E38 de comparaison pour entrer dans un état E40 de génération d'une nouvelle valeur de référence Code-UMCA.

On sort automatiquement de cet état E40 de génération pour entrer dans un état E50 de génération d'un signal électrique de validation SIG-VAL du signal d'accès au périphérique P.

Ensuite, et automatiquement, on quitte cet état E50 de génération du signal électrique de validation SIG-VAL pour entrer dans un état E60 dans lequel on attend que l'accès au périphérique P ait effectivement lieu.

Lorsque dans cet état E60 d'attente on détecte que l'accès a effectivement eu lieu (transition E65), on entre dans un état E70 dans lequel on inhibe le signal de validation SIG-VAL.

On sort ensuite automatiquement de cet état E70 d'inhibition pour retourner à l'état d'attente E20 décrit précédemment.

Dans un autre mode de réalisation, lorsque dans l'état E60 d'attente on détecte l'obtention d'un code dans le registre 21 (transition E67), on entre dans l'état E100 de déclenchement d'une interruption non masquable d'alarme NMI2, ce code d'autorisation d'accès ayant nécessairement été envoyé à l'unité matérielle de contrôle d'accès par un tiers mal intentionné. Ce mode de réalisation permet de renforcer la sécurité du système en détectant des accès frauduleux au périphérique après la validation de l'accès (état E60).

La **figure 4b** représente un diagramme d'état d'un procédé de contrôle d'accès conforme à l'invention dans un deuxième mode de réalisation.

Ce mode de réalisation de l'invention, est simplifié dans le sens, où il ne comporte pas d'étape E25 de réception d'un code de déclenchement Code-DD. Bien entendu toute étape (E30, E31, E32, E85) de traitement de ce code de déclenchement Code-DD est supprimée.

L'étape E25 est remplacée par une étape E26 de déclenchement, celui-ci pouvant se réaliser par tout moyen connu de l'homme du métier susceptible de générer une interruption.

L'étape E26 de déclenchement est suivie automatiquement par l'étape E34 de génération d'une interruption non masquable NMI1 de contrôle décrite en référence à la figure 4a.

Dans ce mode de réalisation, le code d'autorisation Code-AA étant une constante, l'étape E40 de génération d'une valeur de référence Code-UMCA est supprimée.

La routine d'interruption de contrôle IRT1 présente dans le registre 21 la valeur mémorisée par le programme informatique PROG dans la mémoire protégée.

Nous allons maintenant décrire en référence à la **figure 4c** un troisième mode de réalisation du procédé de contrôle d'accès conforme à l'invention.

Dans ce mode de réalisation, on ne vérifie pas, auprès du processeur, que le code d'autorisation d'accès Code-UMCA obtenu en provenance du programme informatique PROG (transition E25) est un code certifié par le processeur.

Ainsi, il n'est pas généré d'interruption non masquable de contrôle NMI1, l'accès au périphérique étant automatiquement validé lorsque le code d'autorisation d'accès Code-AA est identique à la valeur de référence prédéterminée Code-UMCA (transition E31).

L'exécution de ce procédé simplifié est donc plus rapide, le cycle de contrôle étant supprimé.

Préférentiellement, ce troisième mode de réalisation ne comporte pas non plus de génération d'une interruption non masquable d'alarme (E100) en cas d'attaque frauduleuse, mais entraîne un retour dans l'état d'attente E20.

Ainsi, et plus précisément, ce troisième mode de réalisation est identique au premier décrit en référence à la figure 4a, à la différence près que :

- elle ne comporte pas d'état E100 de déclenchement d'une interruption non masquable d'alarme NMI2, et lorsque dans l'état E30 de comparaison, on détermine que le code d'autorisation d'accès Code-AA est différent de la valeur de référence prédéterminée Code-UMCA, on retourne à l'état d'attente E20 ;

- les autres transitions (E22, E90 et E67) transitions décrites précédemment en référence à la figure 4a vers cet état E100 de déclenchement d'une interruption non masquable d'alarme sont supprimées ;

- elle ne comporte pas d'état E34 de déclenchement d'une interruption non masquable de contrôle NMI1, l'état E32 de génération d'une valeur de référence Code-UMCA étant automatiquement suivi par l'état E50 de validation d'accès.

L'invention concerne également un quatrième mode de réalisation du procédé de contrôle d'accès conforme à l'invention, identique au troisième mode de réalisation décrit ci-dessus en référence à la figure 4c, à la seule différence près que l'on entre directement dans l'état E50 de validation du signal d'accès SIG-VAL lorsqu'au cours de l'état E30 de comparaison du code d'autorisation d'accès Code-AA avec la valeur de référence Code-UMCA, on détermine que ces deux valeurs sont égales (transition E31). Ce mode de réalisation est représenté par le diagramme d'états finis de la **figure 4d**.

La **figure 5** représente les principales étapes E500 à E520 d'une routine d'interruption non masquable de contrôle IRT1 mise en œuvre par un processeur conforme à l'invention dans un mode préféré de réalisation.

Cette routine est activée lorsque l'unité matérielle de contrôle d'accès 20 génère une interruption non masquable de contrôle NMI1.

La routine IRT1 décrite ici comporte une première étape E500 au cours de laquelle on mémorise dans une variable VA le contenu d'une variable Code-AA comportant le code d'autorisation d'accès du même nom.

Dans le mode de réalisation décrit en référence à la figure 4a l'étape E500 de lecture du code d'autorisation d'accès Code-AA est suivie par une étape E510 au cours de laquelle on génère un nouveau code d'autorisation d'accès Code-AA selon la loi prédéterminée décrite précédemment. Au cours de cette même étape, on mémorise cette nouvelle valeur du code d'autorisation d'accès Code-AA dans la mémoire protégée.

L'étape E510 de génération et de mémorisation du nouveau code d'autorisation d'accès Code-AA est suivie par une étape E520 d'envoi du contenu de la variable VA à l'unité matérielle de contrôle d'accès 20.

Dans le mode de réalisation préféré décrit ici, cette étape d'envoi consiste à écrire le contenu de la variable VA dans le registre 21.

Dans le mode de réalisation décrit en référence à la figure 4b, l'étape E500 de lecture du code d'autorisation d'accès Code-AA est suivie par cette étape E520.

Quoi qu'il en soit, l'étape E520 d'envoi du code d'autorisation d'accès est suivie par une instruction de type IRET connue de l'homme du métier, qui consiste d'une part à effacer la source de l'interruption NMI1 et à revenir de ladite interruption.

Le procédé de gestion d'accès conforme à l'invention comporte, de façon optionnelle, une routine d'interruption d'alarme IRT2 en réponse à une interruption non masquable NMI2 en provenance de l'unité matérielle de contrôle d'accès 20.

Cette interruption non masquable d'alarme consiste essentiellement à générer une alerte et/ou à traiter l'accès non autorisé selon des règles adéquates.

La **figure 6** représente les principales étapes E600 à E630 d'un programme informatique PROG comportant des instructions d'accès à un périphérique P sécurisé conformément à l'invention, dans le mode de réalisation de la figure 4a.

Ce programme informatique comporte deux étapes E600 et E610 identiques ou similaires respectivement aux étapes E500 de lecture du code d'autorisation d'accès, et E510 de génération et de mémorisation d'un code d'autorisation d'accès décrit précédemment en référence à la figure 5.

Ainsi, au cours de ces deux étapes, le programme informatique P mémorise dans une variable VA le contenu du code de déclenchement Code-DD courant, génère selon la loi prédéterminée (loi d'incrémentation) un nouveau de déclenchement Code-DD, et mémorise cette nouvelle valeur dans la mémoire sécurisée partagée avec la routine d'interruption IRT1.

By Express Mail
No.
EV514454583US

Préalablement à chaque étape E630 d'accès au périphérique P, le programme informatique PROG comporte une étape E620 au cours de laquelle on envoie le contenu de la variable VA à l'unité de contrôle matériel d'accès 20, ce qui revient, dans le mode de réalisation décrit ici, à écrire le contenu de cette variable dans le registre 21.

Cette étape E620 d'envoi du code d'autorisation d'accès VA à l'unité de contrôle matériel d'accès 20 est suivie par l'étape E630 d'accès au périphérique P.

Dans une mise en œuvre de l'invention selon le mode de réalisation de la figure 4b, le programme informatique PROG comporte une étape E610' de mémorisation d'une valeur constante dans la mémoire protégée du processeur, puis une étape E620' de déclenchement de la première interruption de contrôle non masquable IRT1, préalablement à l'étape E630 d'accès au périphérique.

Après l'accès, une valeur quelconque différente de ladite constante est mémorisée dans la mémoire protégée du processeur.

Cette étape peut également être réalisée par la routine d'interruption de contrôle IRT1.

By Express Mail
No. EV514454583US

REVENDICATIONS

1 – Unité matérielle de contrôle d'accès (20) à un périphérique (P), caractérisée en ce qu'elle comporte :

- des moyens (21) d'obtention d'un code d'autorisation d'accès (Code-AA) audit périphérique (P) ;

- des moyens (22) de comparaison dudit code d'autorisation d'accès (Code-AA) avec une valeur de référence prédéterminée (Code-UMCA) ; et

- des moyens dits de validation (22, 23, 25) adaptés à générer un signal électrique de validation (SIG_VAL) d'un signal électrique d'accès (CS, WE, PWR) audit périphérique (P) en fonction du résultat de ladite comparaison.

2 - Unité matérielle de contrôle d'accès selon la revendication 1, caractérisé en ce quelle comporte des moyens (26) de déclenchement d'une interruption non masquable d'alarme (NMI2), lorsque ledit code d'autorisation d'accès (Code-AA) est différent de la valeur de référence prédéterminée (Code-UMCA).

3 – Unité matérielle de contrôle d'accès selon la revendication 1 ou 2, caractérisée en ce que ladite valeur de référence prédéterminée (Code-UMCA) est une constante.

4 - Unité matérielle de contrôle d'accès selon la revendication 1 ou 2, caractérisée en ce qu'elle comporte des moyens (24) de génération de ladite valeur de référence (Code-UMCA) selon une loi prédéterminée.

5 - Unité matérielle de contrôle d'accès selon la revendication 4, caractérisée en ce que ladite valeur de référence prédéterminée (Code-UMCA) est un compteur initialisé à la mise sous tension de ladite unité matérielle (UMCA), et en ce que ladite loi prédéterminée consiste à incrémenter ledit compteur à chaque obtention dudit code d'autorisation d'accès (Code-AA).

6 - Unité matérielle de contrôle d'accès selon l'une quelconque des revendications 1 à 5, caractérisée en ce qu'elle comporte :

- des moyens (26) de déclenchement d'une interruption non masquable de contrôle (NMI1) et;

- des moyens (21) d'obtention dudit code d'autorisation d'accès (Code-AA) consécutivement audit déclenchement.

By Express Mail
No. EV514454583US

7 - Unité matérielle de contrôle d'accès selon l'une quelconque des revendications 1 à 6, caractérisée en ce que lesdits moyens de validation (22, 23, 25) comportent des moyens de combinaison logique (25) adaptés à :

- recevoir un signal électrique de demande d'accès (CS-RQ, WE-RQ) audit périphérique (P) ;

- recevoir ledit signal de validation (SIG_VAL) ; et

- valider ledit signal électrique d'accès (CS, WE) en fonction d'un état (RQ_0, RQ_1) dudit signal électrique de demande d'accès (CS-RQ, WE-RQ), d'un état (VAL_0, VAL_1) dudit signal de validation, et d'une logique représentée dans une table de vérité (25).

8 - Unité matérielle de contrôle d'accès selon la revendication 7, caractérisée en ce qu'elle comporte des moyens (26) de lecture d'un état (RQ_0, RQ_1) dudit signal électrique de demande d'accès (CS_RQ, WE_RQ), et des moyens (26) de déclenchement d'une interruption non masquable d'alarme (NMI2) en fonction de cet état (RQ_0, RQ_1) et dudit état (VAL_0, VAL_1) dudit signal électrique de validation d'accès (SIG_VAL).

9 - Unité matérielle de contrôle d'accès selon l'une quelconque des revendications 1 à 8, caractérisée en ce qu'elle comporte des moyens d'inhibition (23) dudit signal de validation (SIG_VAL).

10 – Unité matérielle de contrôle d'accès selon la revendication 9, caractérisé en ce que lesdits moyens d'inhibition (23) sont adaptés à inhiber ledit signal de validation (SIG_VAL) consécutivement à au moins un accès audit périphérique (P).

11 – Unité matérielle de contrôle d'accès selon la revendication 9 ou 10, caractérisée en ce que lesdits moyens d'inhibition (23) sont adaptés à inhiber ledit signal de validation (SIG_VAL) après un délai prédéterminé compté à partir de la génération dudit signal électrique de validation d'accès (SIG_VAL), où à partir de l'obtention dudit code d'accès (Code-AA).

12 - Processeur (110) caractérisé en ce qu'il comporte une unité matérielle de contrôle d'accès (20) selon l'une quelconque des revendications 1 à 11.

By Express Mail
No. EV514454583US

13 - Processeur selon la revendication 12, caractérisé en ce qu'il comporte en outre des moyens (IRT1) d'envoi dudit code d'autorisation d'accès (Code-AA) à ladite unité matérielle de contrôle d'accès (20).

14 – Processeur selon la revendication 13, caractérisé en ce qu'il comporte en outre des moyens de lecture dudit code d'accès (Code-AA) à partir d'une mémoire protégée en vue dudit envoi.

15 - Processeur selon la revendication 13, caractérisé en ce qu'il comporte en outre des moyens (VECT) de mise en œuvre- d'une routine d'interruption de contrôle (IRT1) adaptée à générer ledit code d'accès (Code-AA) selon une loi prédéterminée, en vue dudit envoi

16 - Processeur selon la revendication 15, caractérisé en ce que ledit code d'accès (Code-AA) est un compteur et en ce que ladite loi prédéterminée consiste à initialiser ledit compteur (Code-AA) lors de la mise sous tension dudit processeur (110), et à incrémenter ledit compteur à chaque envoi dudit code (Code-AA) à ladite unité matérielle (20).

17 - Processeur selon l'une quelconque des revendications 12 à 16, caractérisé en ce qu'il comporte en outre des moyens (VECT) de mise en œuvre d'une routine d'interruption d'alarme (IRT2) adaptée à générer une alerte et/ou à inhiber l'utilisation dudit périphérique (P).

18 – Processeur selon l'une quelconque des revendications 12 à 17, caractérisé en ce qu'il comporte ledit périphérique (P), celui-ci pouvant notamment être choisi parmi un contrôleur d'écriture dans une mémoire d'amorçage (120) dudit processeur, une unité de gestion de mémoire (MMU).

19 - Procédé de contrôle d'accès à un périphérique (P), caractérisé en ce qu'il comporte les étapes suivantes :

- obtention (E37) d'un code d'autorisation d'accès (Code-AA) audit périphérique (P) ;

- comparaison (E38) dudit code d'autorisation d'accès (Code-AA) avec une valeur de référence prédéterminée (Code-UMCA) ;

- génération (E50) d'un signal électrique de validation (SIG_VAL) d'un signal d'accès (CS, WE, PWR) audit périphérique (P) en fonction du résultat de ladite étape de comparaison (E30).

20 - Procédé de contrôle d'accès selon la revendication 19 caractérisé en ce qu'elle comporte une étape (E100), de déclenchement d'une interruption non masquable d'alarme (NMI2) lorsque ledit code d'autorisation d'accès (Code-AA) est différent de la valeur de référence prédéterminé (Code UMCA).

21 – Procédé de contrôle d'accès selon la revendication 19 ou 20, caractérisée en ce que ladite valeur de référence prédéterminée (Code-UMCA) est une constante.

22 - Procédé de contrôle d'accès selon la revendication 19 ou 20 caractérisé en ce qu'il comporte en outre une étape (E40) de génération de ladite valeur de référence (Code-UMCA) selon une loi prédéterminée.

23 - Procédé de contrôle d'accès selon la revendication 22, caractérisé en ce que ladite valeur de référence prédéterminée (Code-UMCA) étant un compteur, il comporte en outre une étape de d'initialisation (E10) dudit compteur, et en ce que ladite étape (E40) de génération, consiste à incrémenter ledit compteur (Code-UMCA) à chaque obtention dudit code d'autorisation d'accès (Code-AA).

24 - Procédé de contrôle d'accès selon l'une quelconque des revendications 19 à 23, caractérisé en ce qu'il comporte en outre :

- une étape (E34) de déclenchement d'une interruption non masquable de contrôle (NMI1) ; et

- une étape (E37) d'obtention dudit code d'accès (Code-AA) consécutivement audit déclenchement.

25 – Procédé de contrôle d'accès selon la revendication 24, caractérisé en ce que ladite étape de déclenchement (E34) est effectuée consécutivement à une étape d'obtention (E25) d'un code de déclenchement (Code-DD).

26 - Procédé de contrôle d'accès selon l'une quelconque des revendications 19 à 25, caractérisé en ce que, au cours de ladite étape (E50) de génération du signal de validation :

- on lit l'état (RQ_0, RQ_1) d'un signal électrique (CS-RQ, WE-RQ) de demande d'accès audit périphérique (P) ;

- on lit l'état (VAL_0, VAL_1) dudit signal de validation (SIG_VAL) ; et

- on valide ledit signal électrique d'accès (CS, WE) en fonction dudit état (RQ_1) dudit signal électrique de demande d'accès (CS_RQ, WE_RQ), dudit

état (VAL_1) du signal de validation (SIG_VAL), et en fonction d'une règle logique.

27 - Procédé de contrôle d'accès selon la revendication 26, caractérisé en ce qu'il comporte une étape (E20, E36) de lecture d'un état (RQ_0, RQ_1) dudit signal électrique de demande d'accès (CS_RQ, WE_RQ), et une étape (E100) de déclenchement d'une interruption non masquable d'alarme (NMI2) en fonction dudit état (RQ_0, RQ_1) et dudit état (VAL_0, VAL_1) dudit signal électrique de validation d'accès (SIG_VAL).

28 - Procédé de contrôle d'accès selon l'une quelconque des revendications 19 à 27, caractérisé en ce qu'il comporte une étape (E70) d'inhibition dudit signal de validation (SIG_VAL).

29 – Procédé de contrôle d'accès selon la revendication 28, caractérisé en ce que ladite étape (E70) d'inhibition est effectuée consécutivement à au moins une étape d'accès (E65) audit périphérique (P).

30 – Procédé de contrôle d'accès selon la revendication 28 ou 29, caractérisé en ce que ladite étape d'inhibition est effectuée après un délai prédéterminé compté à partir de ladite étape (E50) de génération du signal de validation (SIG_VAL) ou à partir de l'étape (E25) d'obtention dudit code de déclenchement (Code-DD).

31 – Procédé de gestion d'accès à un périphérique (P), caractérisé en ce qu'il comporte une étape de mise en œuvre d'une routine (IRT1) associée à une interruption non masquable de contrôle (NMI1), ladite routine de contrôle comportant une étape (E520) d'envoi d'un code d'autorisation d'accès (Code-AA) à une unité matérielle de contrôle d'accès (20) conforme à l'une quelconque des revendications 1 à 11.

32 – Procédé de gestion d'accès à un périphérique (P) selon la revendication 31, caractérisé en ce qu'il comporte une étape de lecture dudit code d'accès (Code-AA) à partir d'une mémoire protégée en vue dudit envoi.

33 – Procédé de gestion d'accès à un périphérique (P) selon la revendication 31, caractérisé en ce qu'il comporte une étape (E510) de génération, selon une loi prédéterminée, d'un code d'autorisation d'accès (Code-AA) audit périphérique (P), en vue dudit envoi.

By Express Mail
No. EV514454583US

34 - Procédé de gestion d'accès selon la revendication 33, caractérisé en ce que ledit code d'autorisation d'accès (Code-AA) étant un compteur, il comporte en outre une étape d'initialisation dudit compteur (Code-AA), et en ce que ladite étape (E510) de génération consiste à incrémenter ledit compteur (Code-AA) préalablement à chaque envoi (S100) dudit code d'autorisation d'accès (Code-AA) à ladite unité matérielle (20).

35 - Procédé de gestion d'accès selon l'une quelconque des revendications 31 à 34, caractérisé en ce qu'il comporte en outre une étape de mise en œuvre d'une routine d'interruption non masquable d'alarme (IRT2), ladite routine d'alarme comportant une étape de génération d'une alerte et/ou d'inhibition de l'utilisation dudit périphérique.

36 - Programme informatique comportant une instruction (E630) d'accès à un périphérique (P), caractérisé en ce qu'il comporte une instruction (E620) d'envoi d'un code de déclenchement (Code-DD) à une unité matérielle de contrôle d'accès (20) dudit périphérique (P) conforme à l'une quelconque des revendications 1 à 11, préalablement à l'exécution de ladite instruction d'accès.

37 - Programme informatique selon la revendication 36, caractérisé en ce qu'il comporte en outre des moyens de génération dudit code de déclenchement (Code-DD) selon ladite loi prédéterminée.

38 – Processeur adapté à mettre en œuvre un procédé de contrôle d'accès conforme à l'une quelconque des revendications 19 à 30 et/ou un procédé de gestion d'accès conforme à l'une quelconque des revendications 31 à 35 et/ou un programme informatique conforme à la revendication 36 ou 37.

39 – Utilisation d'une unité matérielle de contrôle d'accès (20) selon l'une quelconque des revendications 1 à 11, pour valider un signal d'accès à un périphérique (P) pouvant notamment être choisi parmi un écran, un clavier, une mémoire, un contrôleur d'une interface de communication, une unité de gestion mémoire (MMU) ou une unité de protection de mémoire (MPU).

By Express Mail
No. EV514454583US

Procédé et dispositif de sécurisation de l'accès à un périphérique.

ABREGE DESCRIPTIF

Ce procédé et ce dispositif (110) de contrôle d'accès à un périphérique permettent la protection de plate-forme électroniques notamment contre les attaques matérielles.

Figure 1.

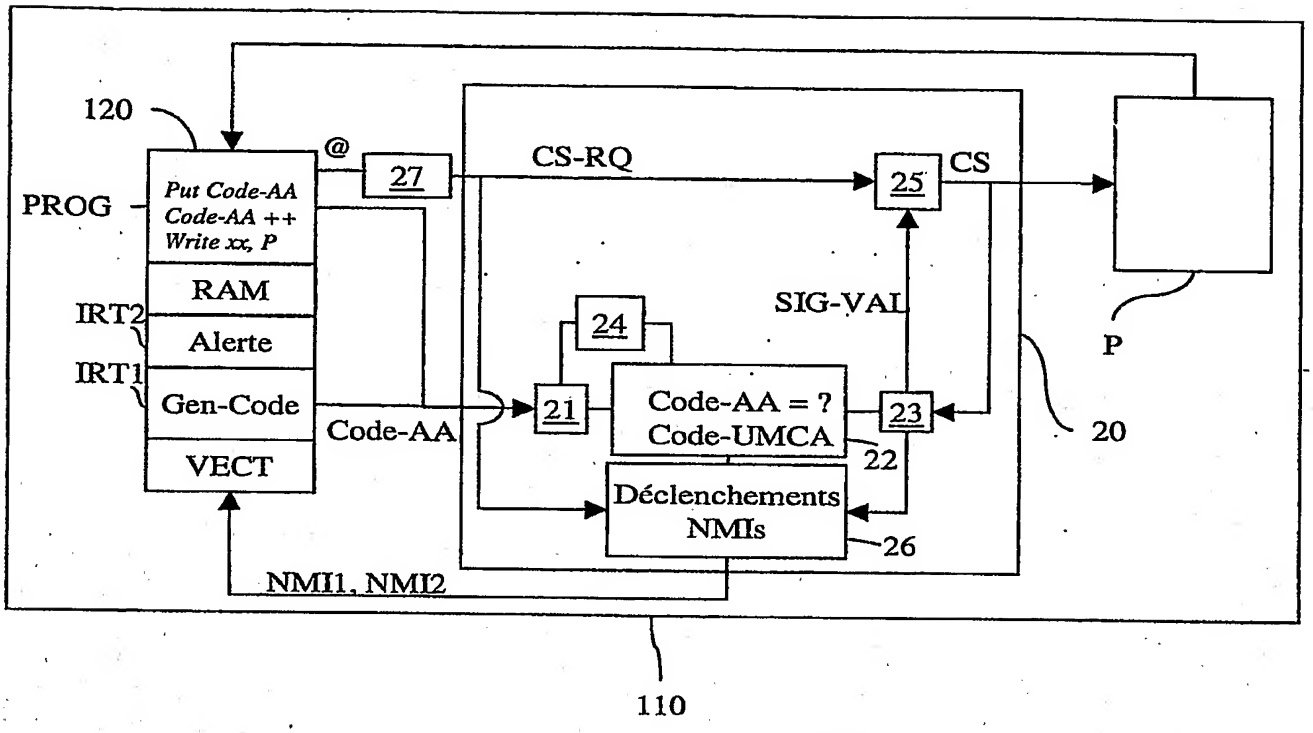

FIG. 1

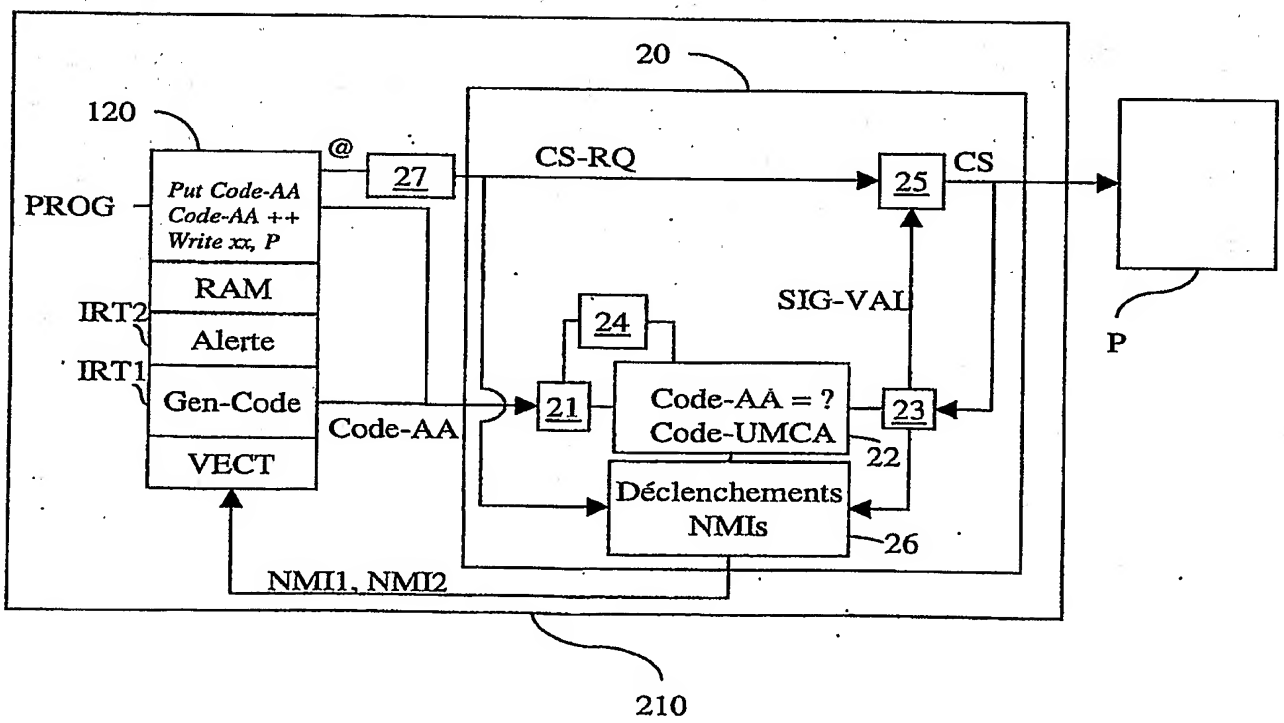

FIG. 2

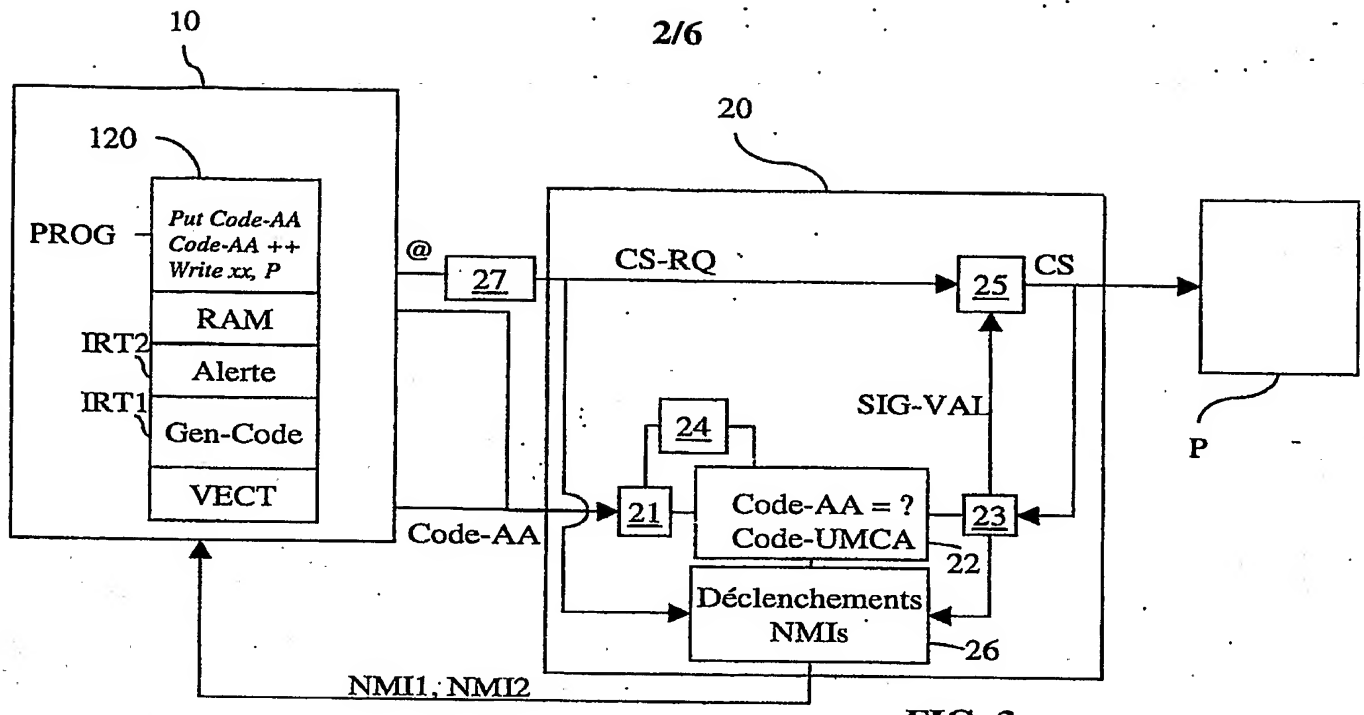

FIG. 3

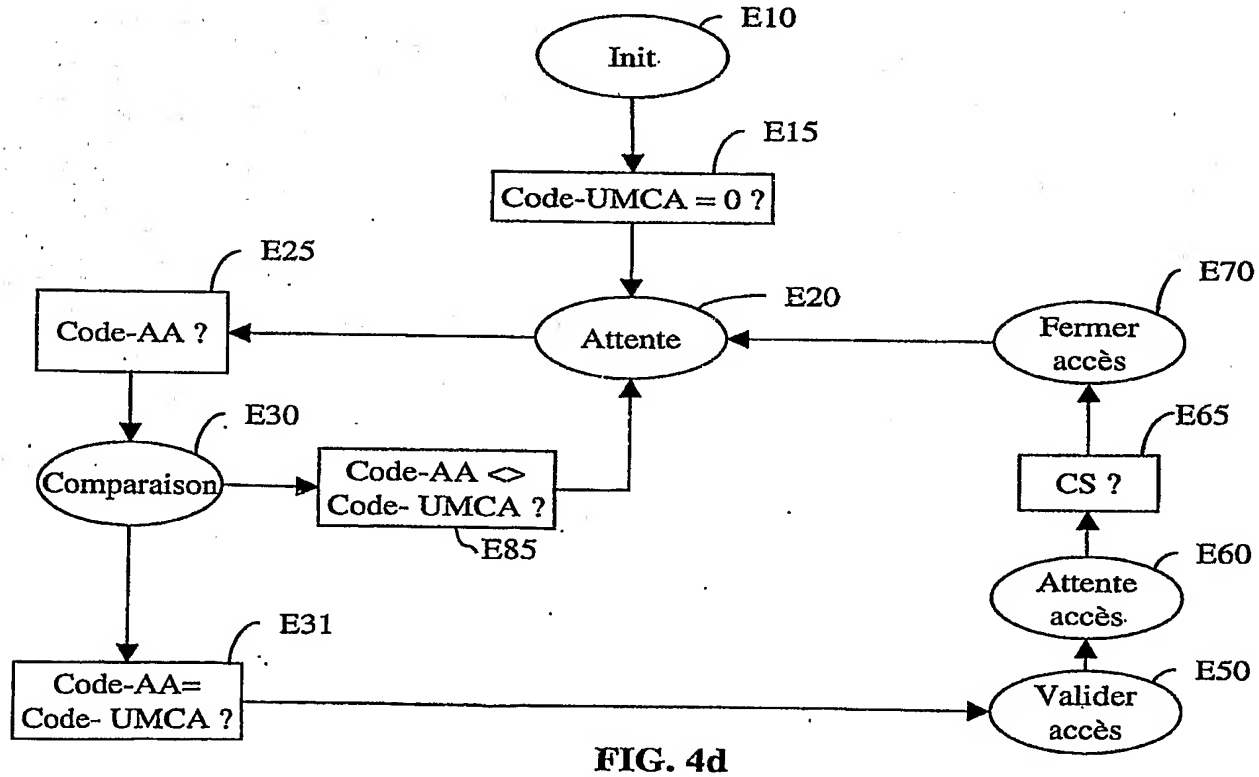

FIG. 4d

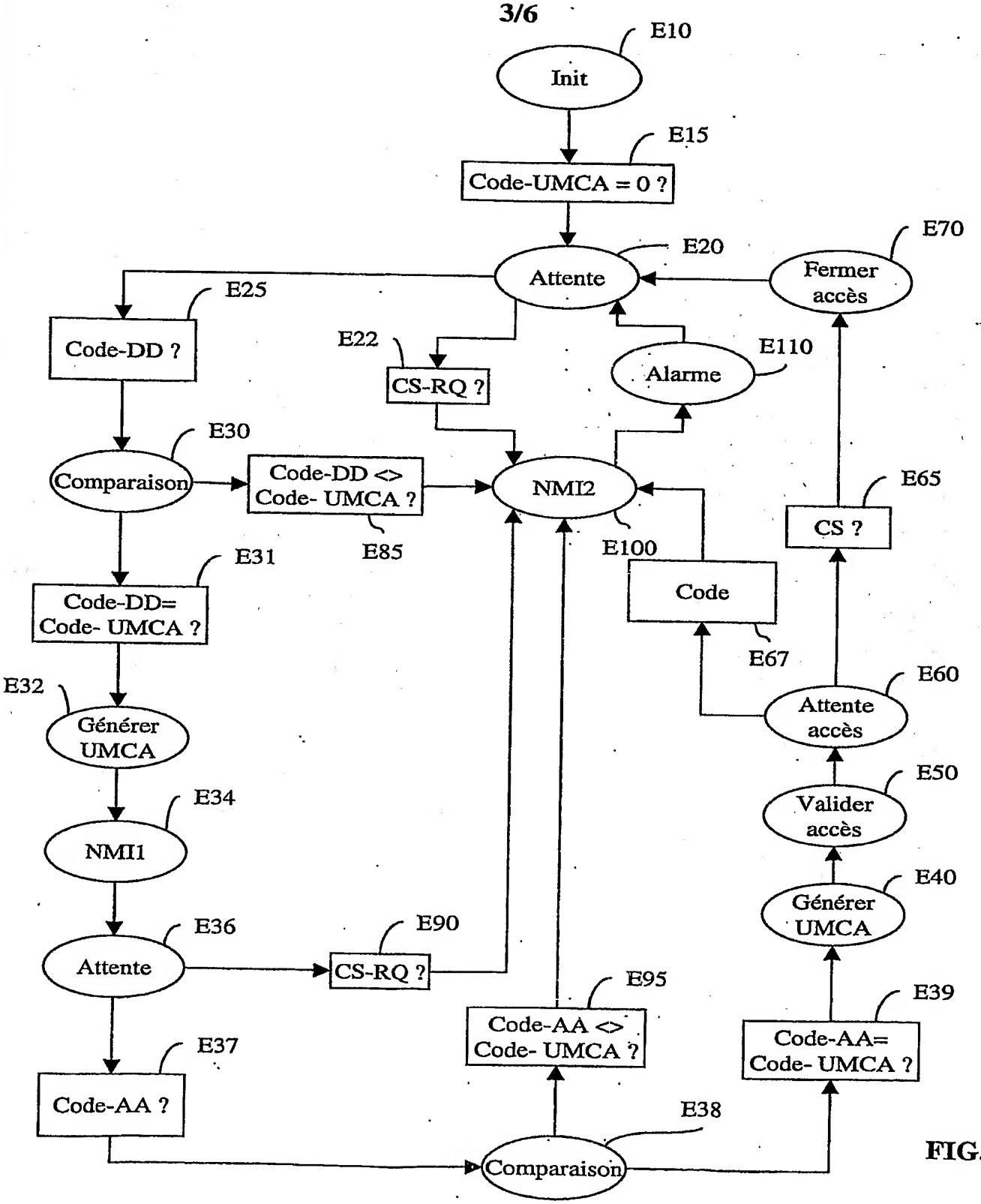

FIG. 4a

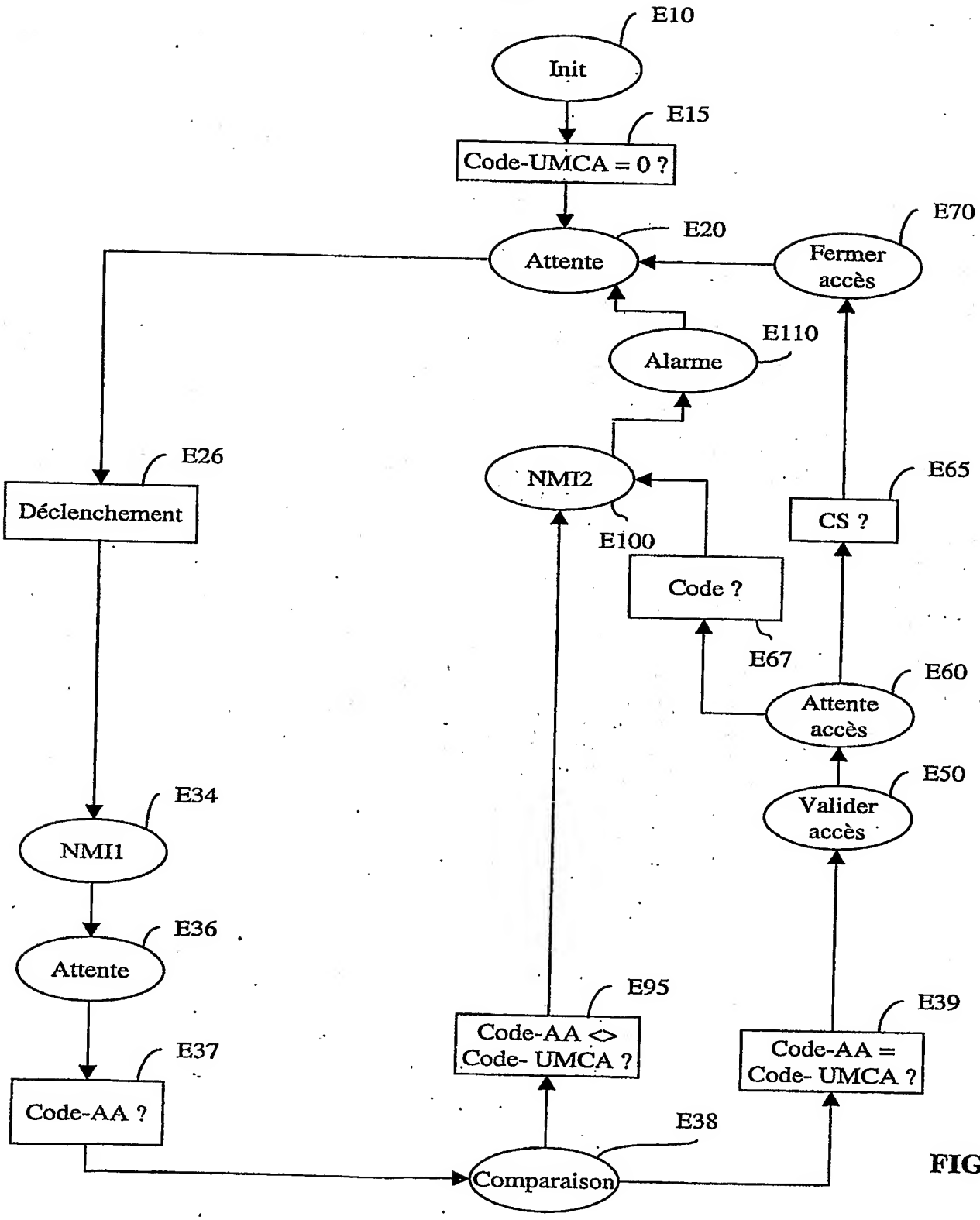

FIG. 4b

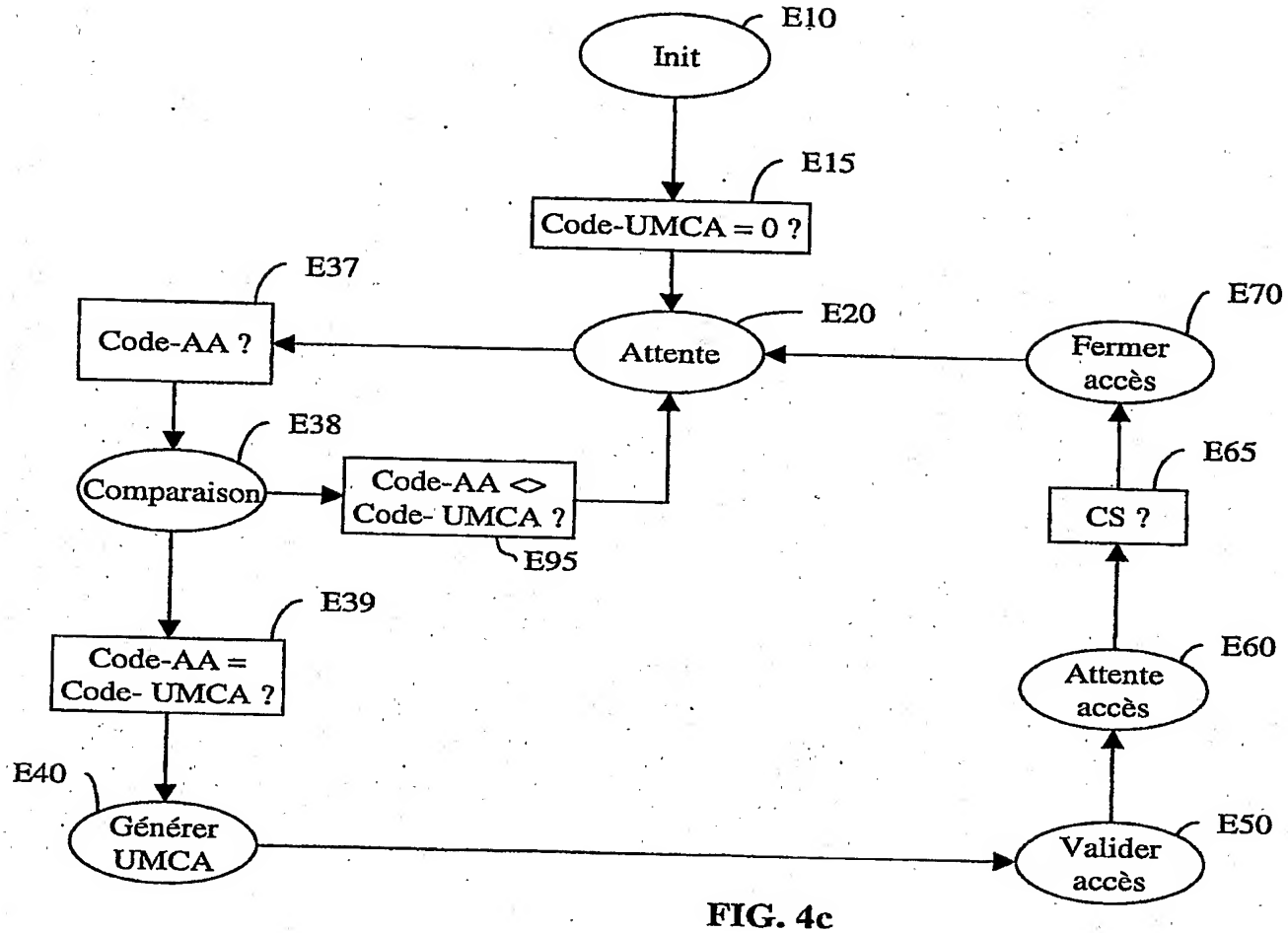

FIG. 4c

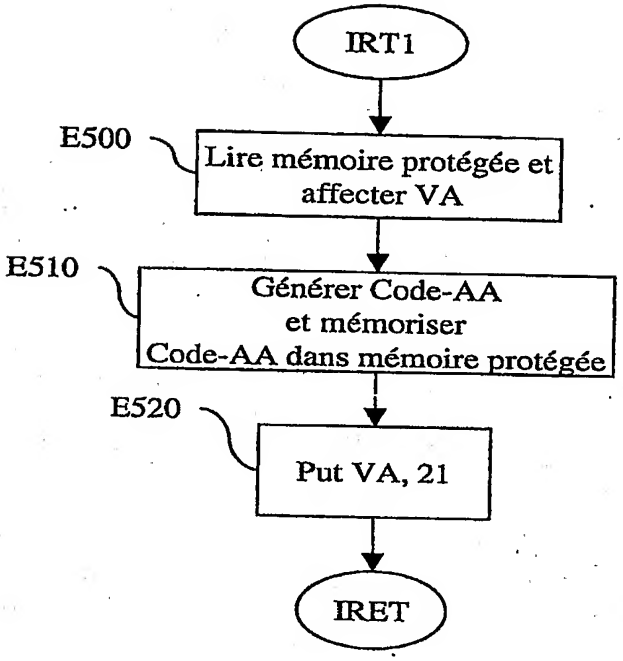

FIG. 5

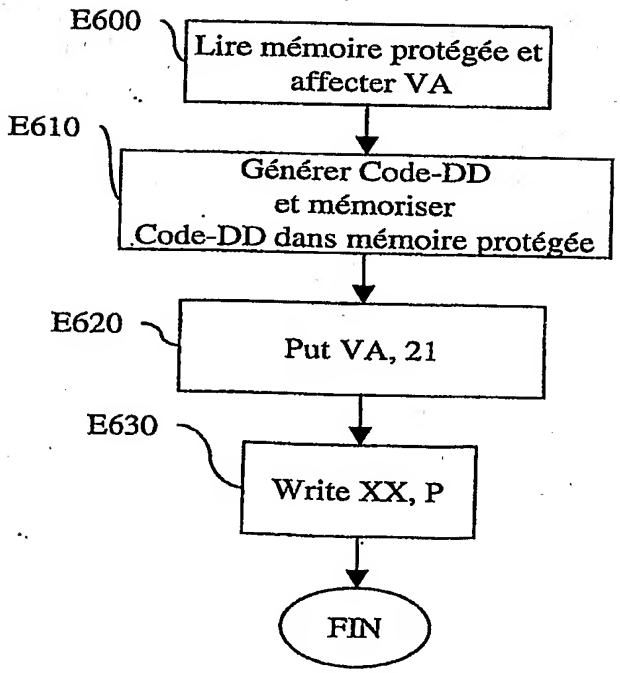

FIG. 6